TR-4955: Disaster Recovery con FSx ONTAP e VMC (AWS VMware Cloud)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-cloud/vmware/vmw-aws-vmc-dro.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommario

TR-4955: Disaster Recovery con FSx ONTAP e VMC (AWS VMware Cloud) . . . 1
- Panoramica . . . 1
- Iniziare . . . 1
  - Distribuisci e configura VMware Cloud su AWS . . . 2
  - Fornire e configurare FSx ONTAP . . . 2
  - Distribuisci e configura SnapMirror su FSx ONTAP . . . 2
- Installazione DRO . . . 3
  - Prerequisiti . . . 3
  - Requisiti OS . . . 3
  - Installa il pacchetto . . . 3
- Configurazione DRO . . . 4
  - Raggruppamenti di risorse . . . 6
  - Piani di replicazione . . . 7
  - Recupero da ransomware . . . 15
- Benefici . . . 15

TR-4955: Disaster Recovery con FSx ONTAP e VMC (AWS VMware Cloud)

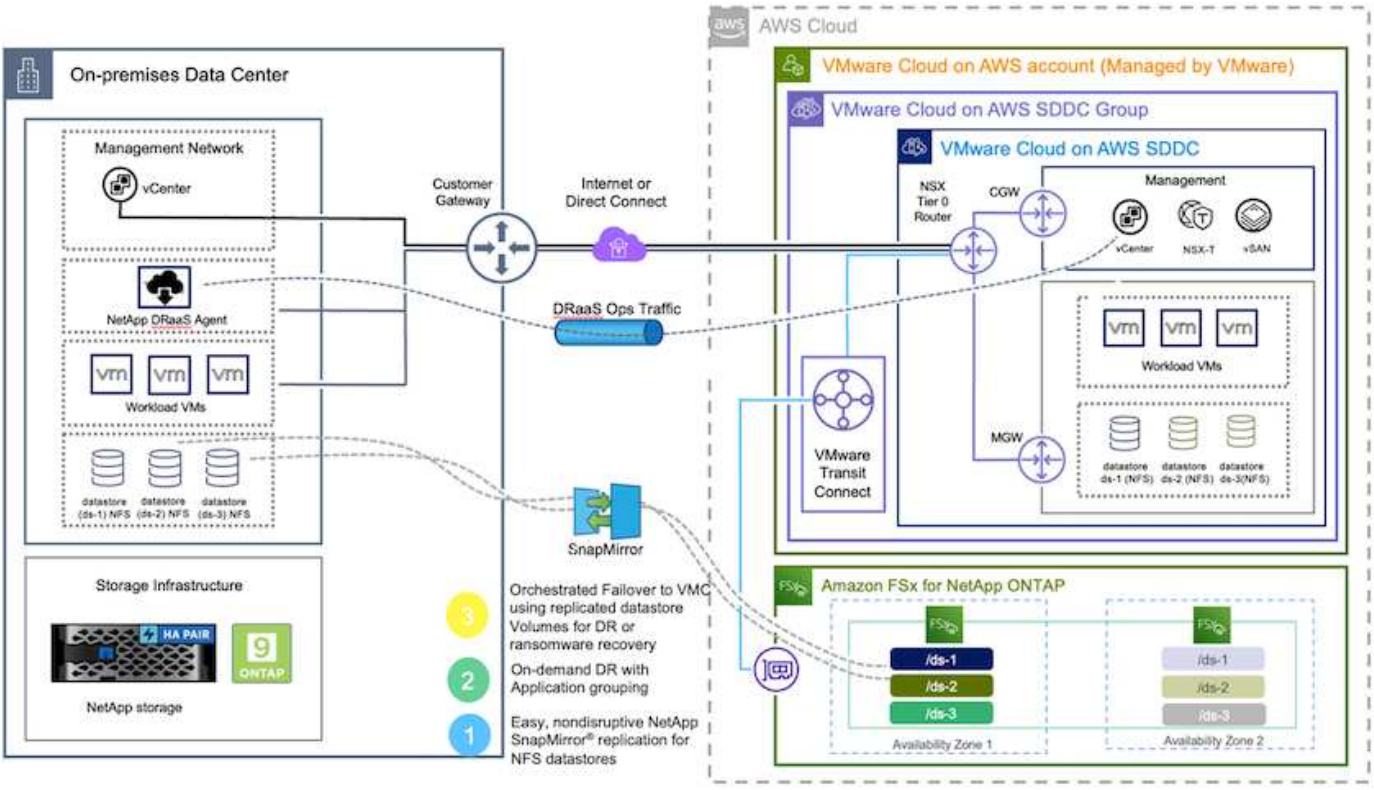
Disaster Recovery Orchestrator (DRO; una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale a FSx ONTAP. DRO automatizza il ripristino dal livello SnapMirror , tramite la registrazione della VM su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzionalità è inclusa in tutti gli ambienti VMC.

Niyaz Mohamed, NetApp

Panoramica

Il disaster recovery nel cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware). Grazie alla tecnologia NetApp SnapMirror , i carichi di lavoro VMware on-premise possono essere replicati su FSx ONTAP in esecuzione su AWS.

Disaster Recovery Orchestrator (DRO; una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale a FSx ONTAP. DRO automatizza il ripristino dal livello SnapMirror , tramite la registrazione della VM su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzionalità è inclusa in tutti gli ambienti VMC.



Iniziare

Distribuisci e configura VMware Cloud su AWS

"VMware Cloud su AWS"fornisce un'esperienza cloud-native per carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni VMware Software-Defined Data Center (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage software-defined vSAN e uno o più host ESXi che forniscono risorse di elaborazione e storage ai carichi di lavoro. Per configurare un ambiente VMC su AWS, seguire i passaggi riportati di seguito"collegamento" . Per scopi DR è possibile utilizzare anche un gruppo di spie luminose.

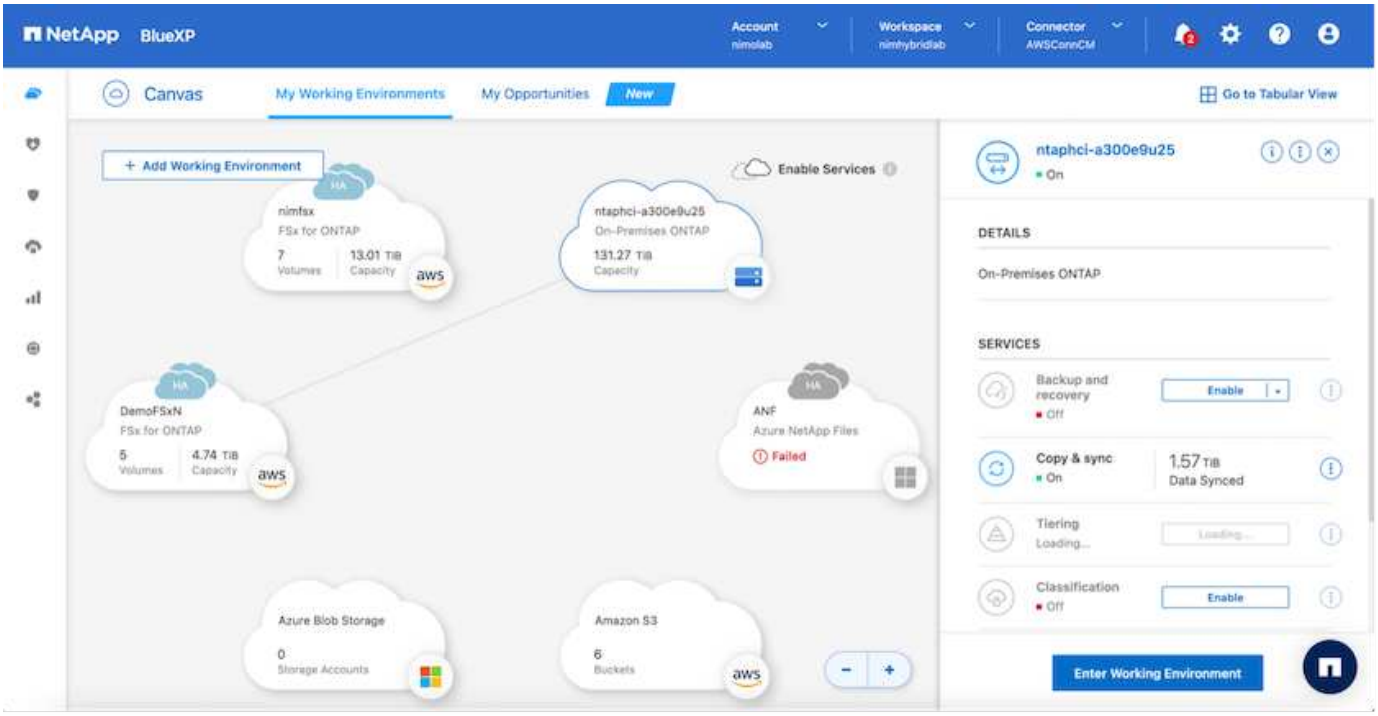
Nella versione iniziale, DRO supporta un cluster di spie luminose esistente. La creazione di SDDC su richiesta sarà disponibile in una prossima versione.

Fornire e configurare FSx ONTAP

Amazon FSx ONTAP è un servizio completamente gestito che fornisce un archivio file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità, basato sul famoso file system NetApp ONTAP . Segui i passaggi qui"collegamento" per fornire e configurare FSx ONTAP.

Distribuisci e configura SnapMirror su FSx ONTAP

Il passaggio successivo consiste nell'utilizzare NetApp BlueXP e individuare l'istanza FSx ONTAP su AWS fornita e replicare i volumi del datastore desiderati da un ambiente locale a FSx ONTAP con la frequenza appropriata e la conservazione delle copie Snapshot NetApp :



Per configurare BlueXP, segui i passaggi indicati in questo link. È anche possibile utilizzare NetApp ONTAP CLI per pianificare la replica seguendo questo collegamento.

Una relazione SnapMirror è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a usare DRO, utilizza il sistema operativo Ubuntu su un'istanza EC2 o una macchina virtuale designata per assicurarti di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti

- Assicurarsi che esista la connettività con i sistemi vCenter e di storage di origine e di destinazione.
- Se si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, è necessario utilizzare indirizzi IP per i sistemi vCenter e di storage.
- Creare un utente con permessi di root. È possibile utilizzare sudo anche con un'istanza EC2.

Requisiti OS

- Ubuntu 20.04 (LTS) con un minimo di 2 GB e 4 vCPU
- I seguenti pacchetti devono essere installati sulla VM dell'agente designata:
  - Docker
  - Docker-compose
  - Jq

Cambia i permessi su `docker.sock` : `sudo chmod 666 /var/run/docker.sock` .

IL `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

Installa il pacchetto

1. Scaricare il pacchetto di installazione sulla macchina virtuale designata:

```
git clone https://github.com/NetApp/DRO-AWS.git
```

   L'agente può essere installato in locale o all'interno di una VPC AWS.

2. Decomprimi il pacchetto, esegui lo script di distribuzione e inserisci l'IP dell'host (ad esempio, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Passare alla directory ed eseguire lo script di distribuzione come segue:

```
sudo sh deploy.sh
```

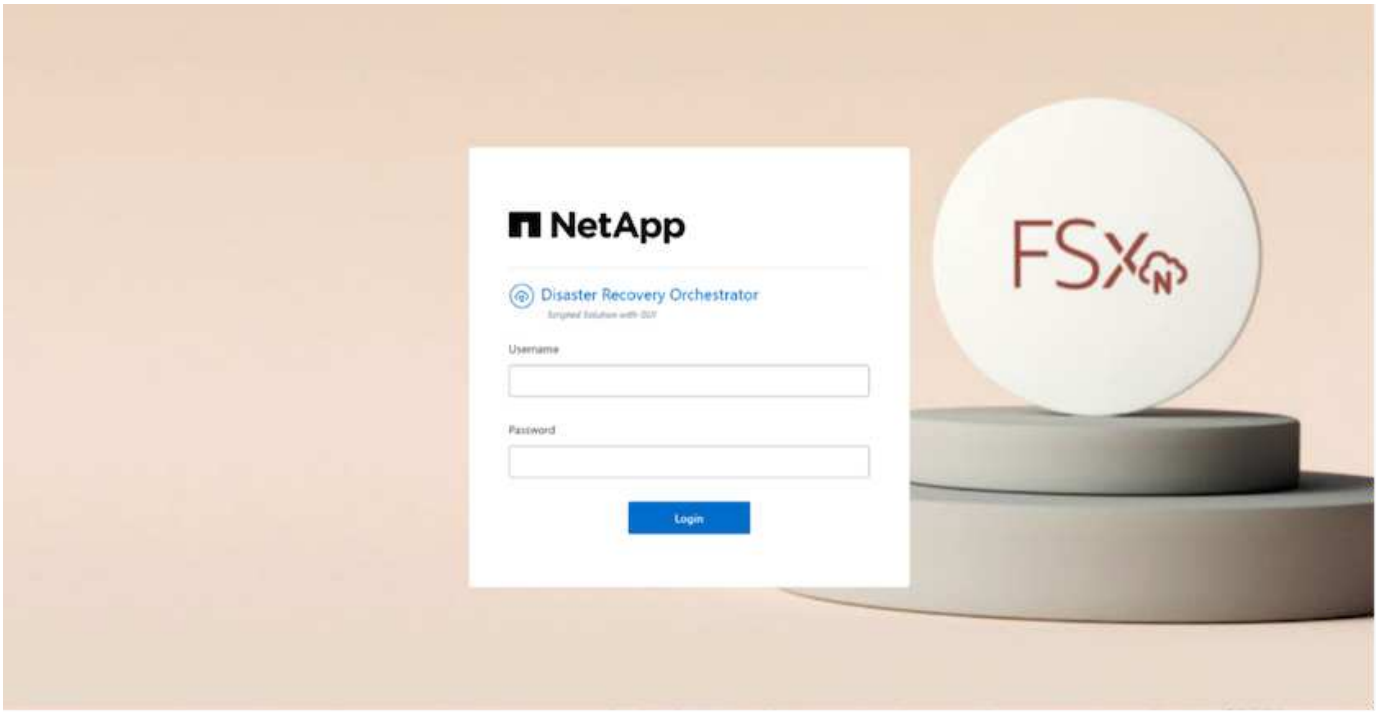
4. Accedi all'interfaccia utente tramite:

```
https://<host-ip-address>
```

con le seguenti credenziali predefinite:

```
Username: admin
Password: admin
```

La password può essere modificata utilizzando l'opzione "Cambia password".



Configurazione DRO

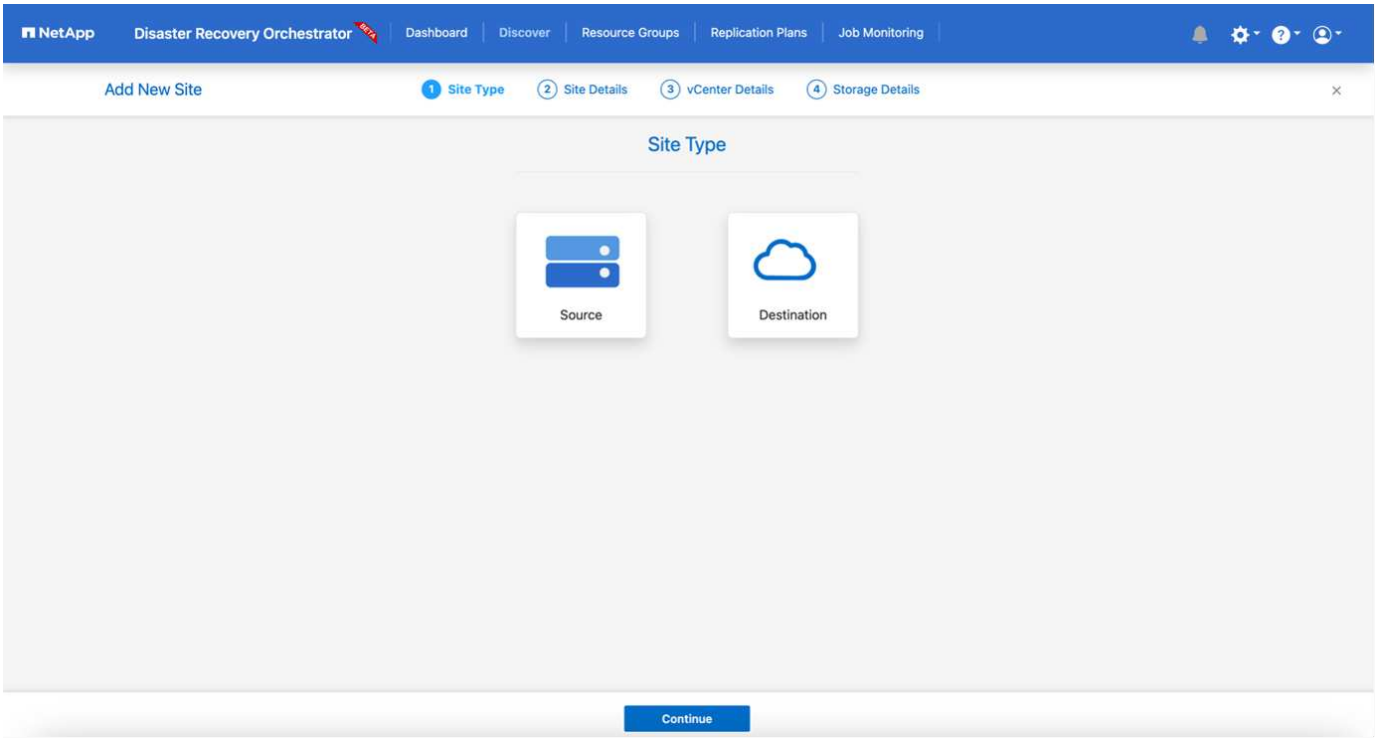
Dopo aver configurato correttamente FSx ONTAP e VMC, è possibile iniziare a configurare DRO per automatizzare il ripristino dei carichi di lavoro locali su VMC utilizzando le copie SnapMirror di sola lettura su FSx ONTAP.

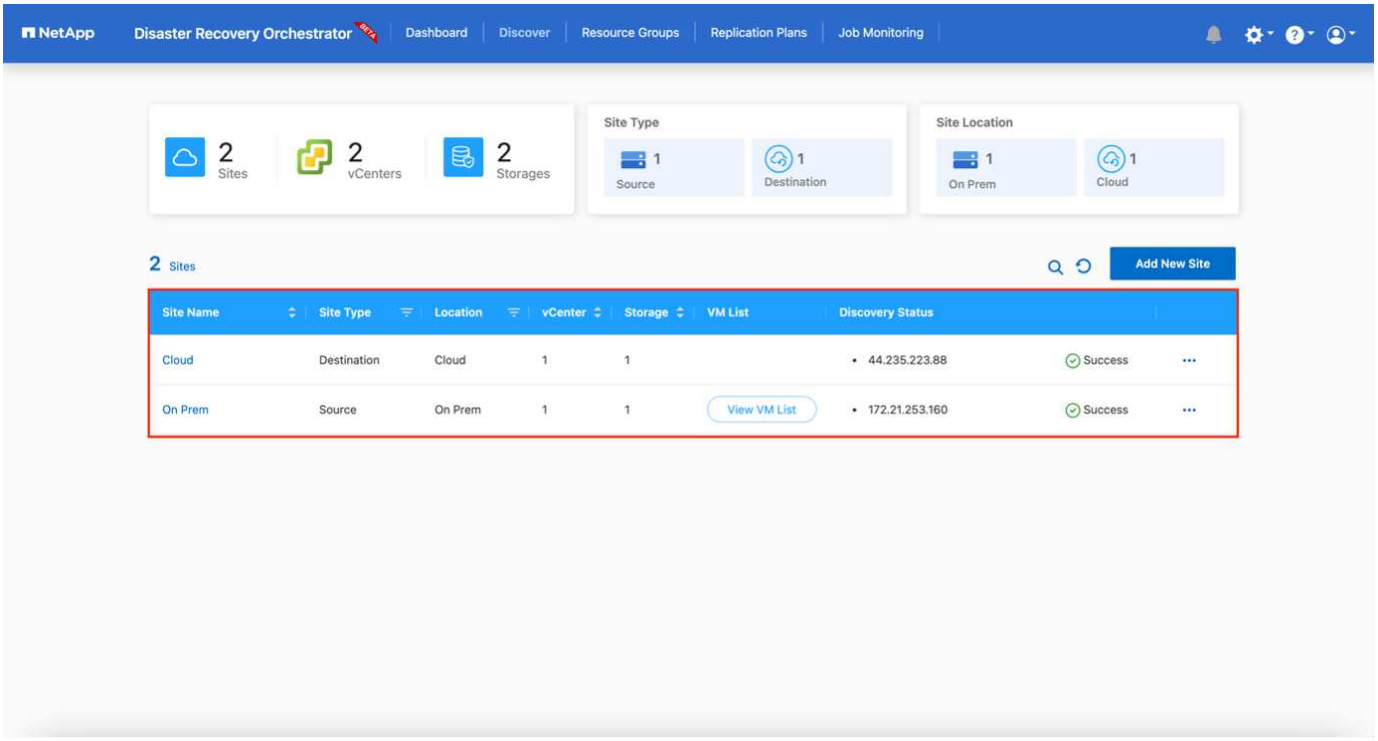
NetApp consiglia di distribuire l'agente DRO in AWS e anche nella stessa VPC in cui è distribuito FSx ONTAP (può anche essere connessa tramite peer), in modo che l'agente DRO possa comunicare tramite la rete con i componenti locali e con le risorse FSx ONTAP e VMC.

Il primo passo è individuare e aggiungere le risorse on-premise e cloud (sia vCenter che storage) a DRO. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (admin/admin) e Aggiungi siti. È possibile aggiungere siti anche tramite l'opzione Scopri. Aggiungere le seguenti piattaforme:

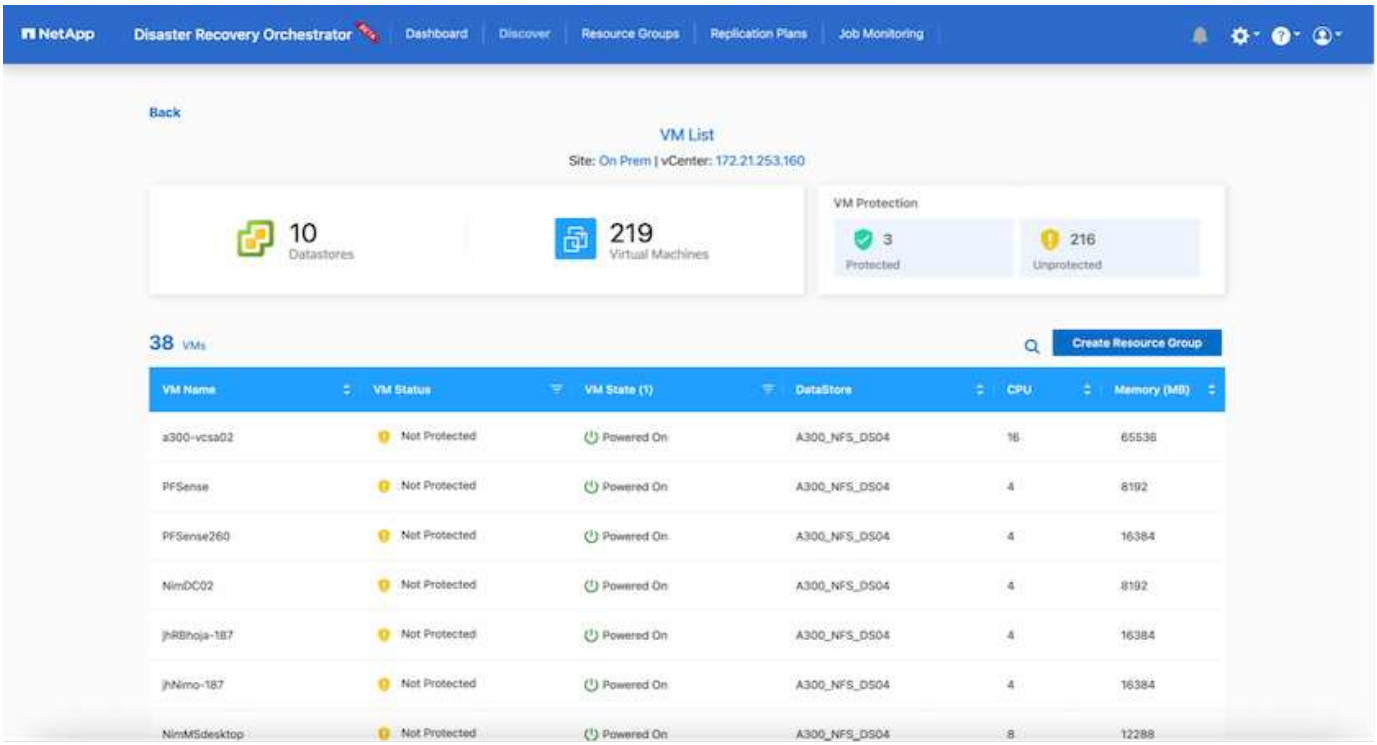
- In sede
  - vCenter locale
  - Sistema di archiviazione ONTAP

- Nuvola
  - VMC vCenter
  - FSx ONTAP





Una volta aggiunto, DRO esegue la rilevazione automatica e visualizza le VM che dispongono delle repliche SnapMirror corrispondenti dall'archiviazione di origine a FSx ONTAP. DRO rileva automaticamente le reti e i gruppi di porte utilizzati dalle VM e li popola.



Il passaggio successivo consiste nel raggruppare le VM necessarie in gruppi funzionali che fungeranno da gruppi di risorse.

Raggruppamenti di risorse

Dopo aver aggiunto le piattaforme, è possibile raggruppare le VM che si desidera ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

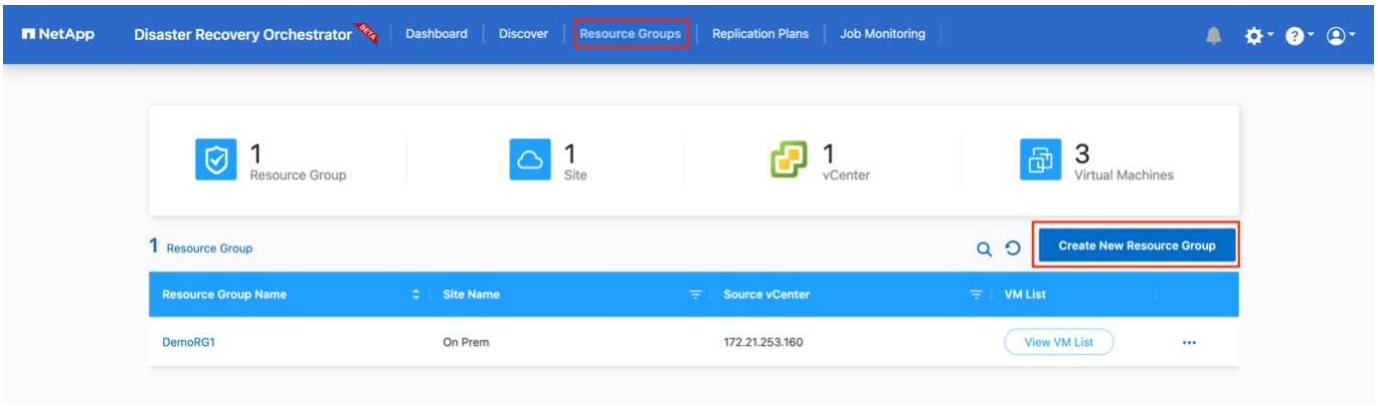
Per iniziare a creare gruppi di risorse, completare i seguenti passaggi:

1. Accedi a **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.
2. In **Nuovo gruppo di risorse**, seleziona il sito di origine dal menu a discesa e fai clic su **Crea**.
3. Fornisci **Dettagli del gruppo di risorse** e fai clic su **Continua**.
4. Selezionare le VM appropriate utilizzando l'opzione di ricerca.
5. Selezionare l'ordine di avvio e il ritardo di avvio (secondi) per le VM selezionate. Imposta l'ordine della sequenza di accensione selezionando ogni VM e impostandone la priorità. Tre è il valore predefinito per tutte le VM.

   Le opzioni sono le seguenti:

   1 – La prima macchina virtuale ad accendersi 3 – Predefinito 5 – L'ultima macchina virtuale ad accendersi

6. Fare clic su **Crea gruppo di risorse**.

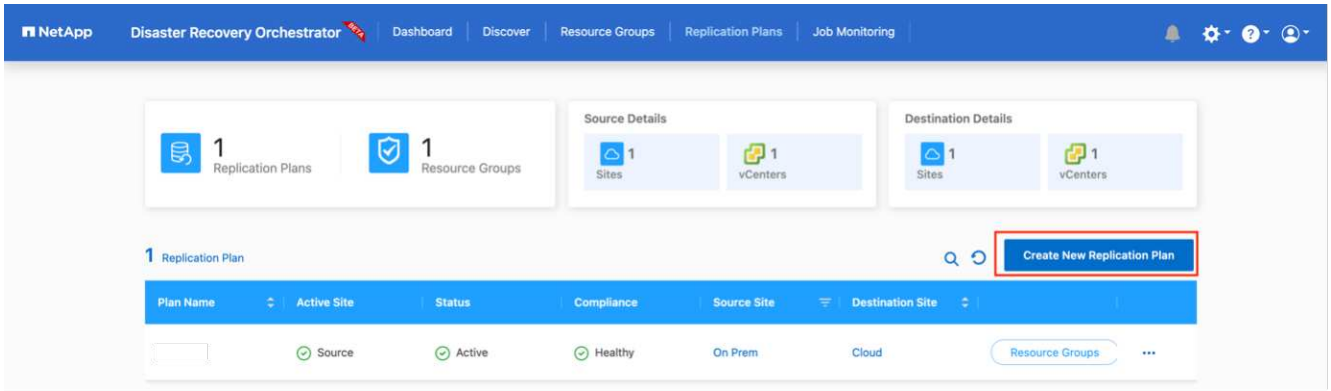


Piani di replicazione

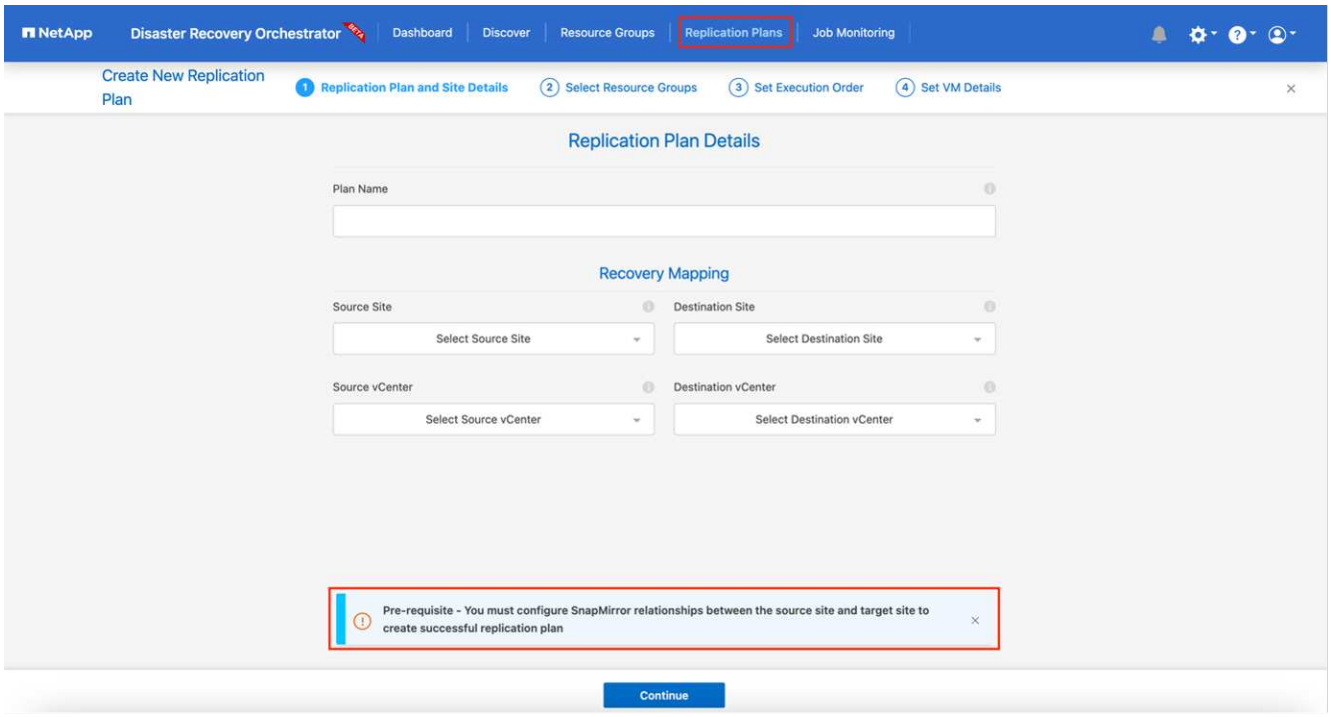
È necessario un piano per ripristinare le applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere in questo piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, quindi livello 1, quindi livello 2 e così via). Tali piani sono talvolta chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Nuovo piano di replica**.

Per iniziare a creare un piano di replicazione, completare i seguenti passaggi:

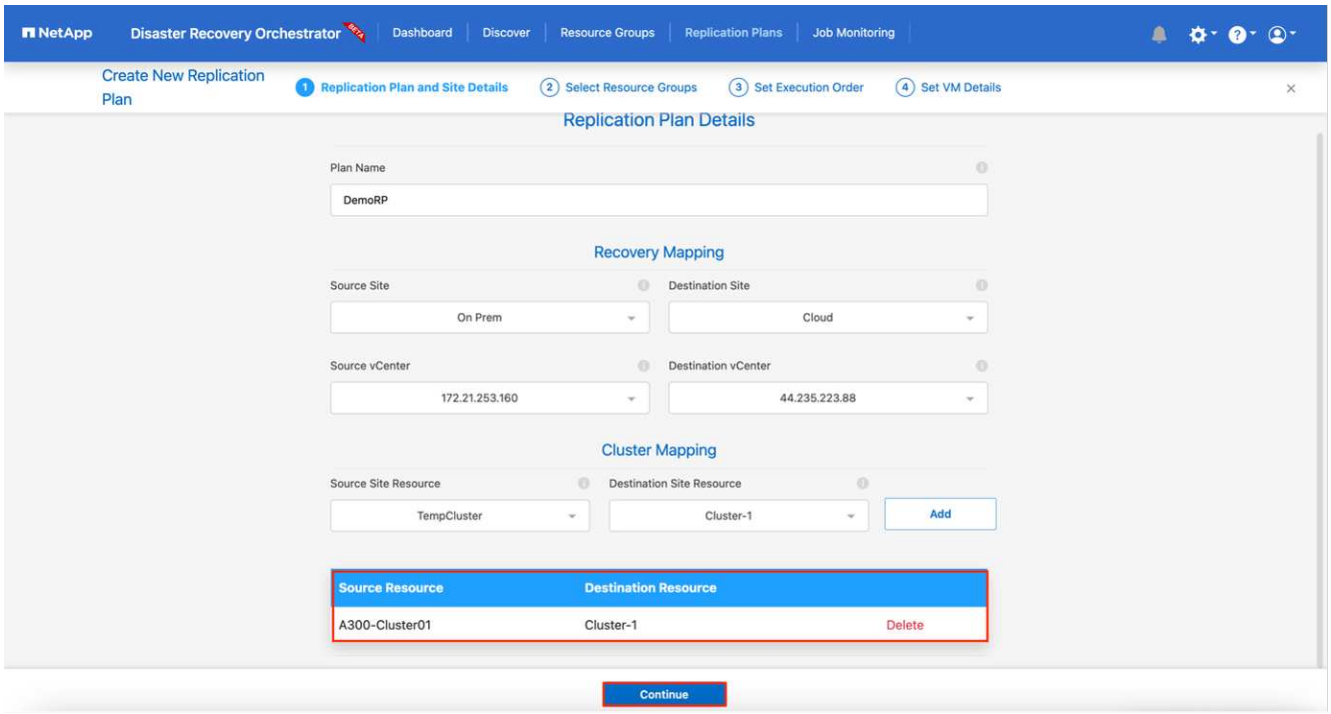
1. Accedi a **Piani di replicazione** e fai clic su **Crea nuovo piano di replicazione**.



2. In **Nuovo piano di replica**, specificare un nome per il piano e aggiungere i mapping di ripristino selezionando il sito di origine, il vCenter associato, il sito di destinazione e il vCenter associato.

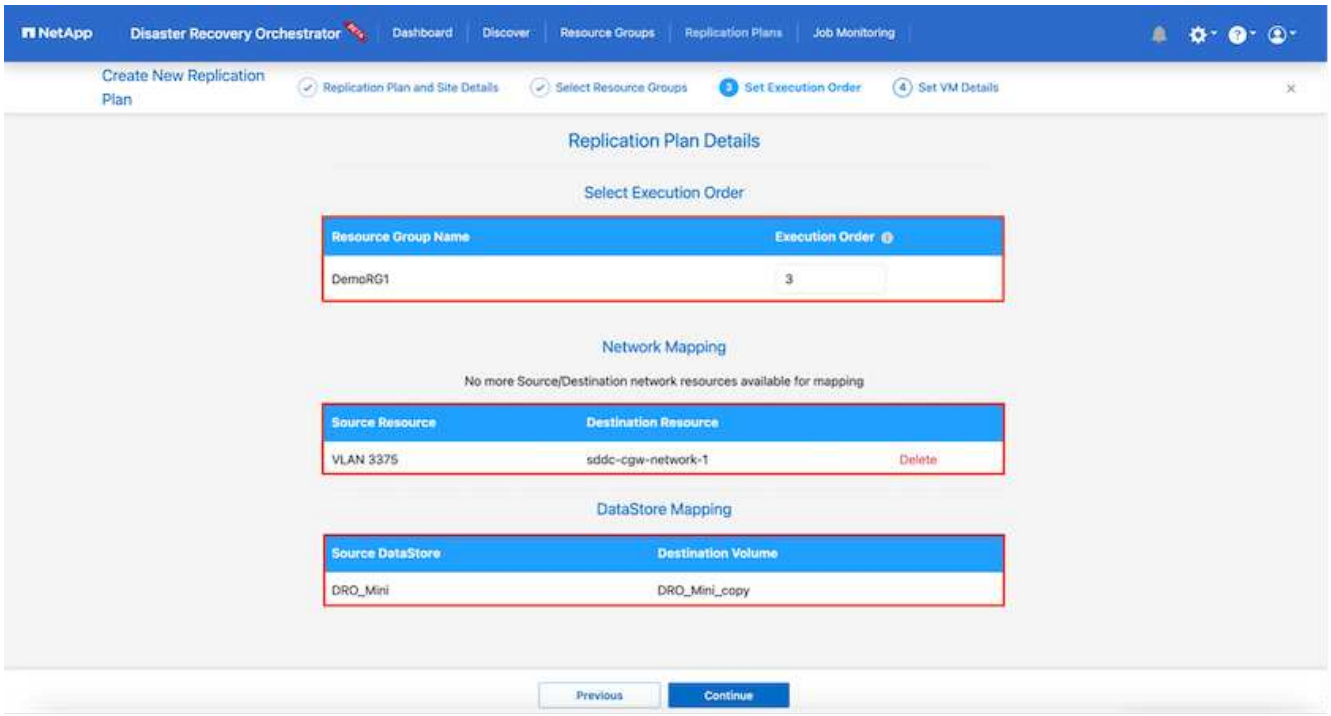


3. Una volta completata la mappatura del ripristino, selezionare la mappatura del cluster.

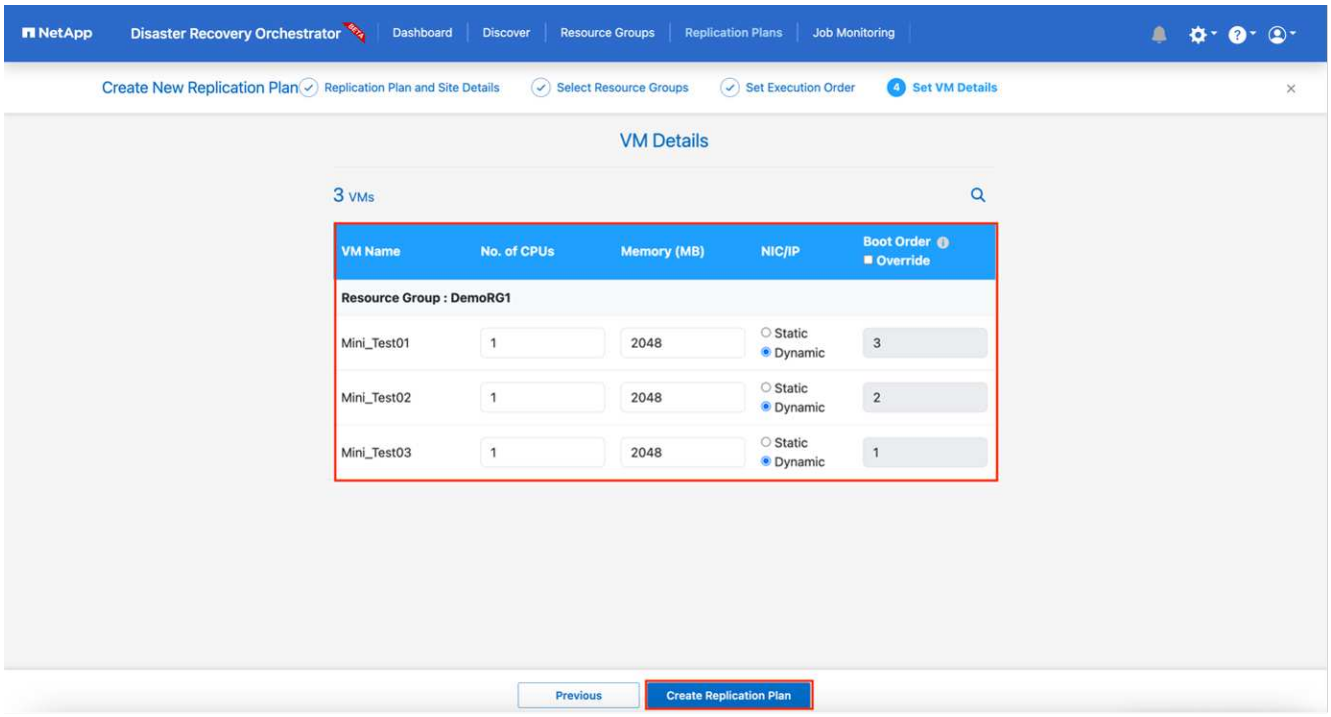


4. Selezionare **Dettagli gruppo di risorse** e fare clic su **Continua**.
5. Imposta l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza delle operazioni quando sono presenti più gruppi di risorse.
6. Una volta terminato, seleziona la mappatura di rete sul segmento appropriato. I segmenti dovrebbero essere già predisposti in VMC, quindi seleziona il segmento appropriato per mappare la VM.
7. In base alla selezione delle VM, vengono selezionate automaticamente le mappature dei datastore.

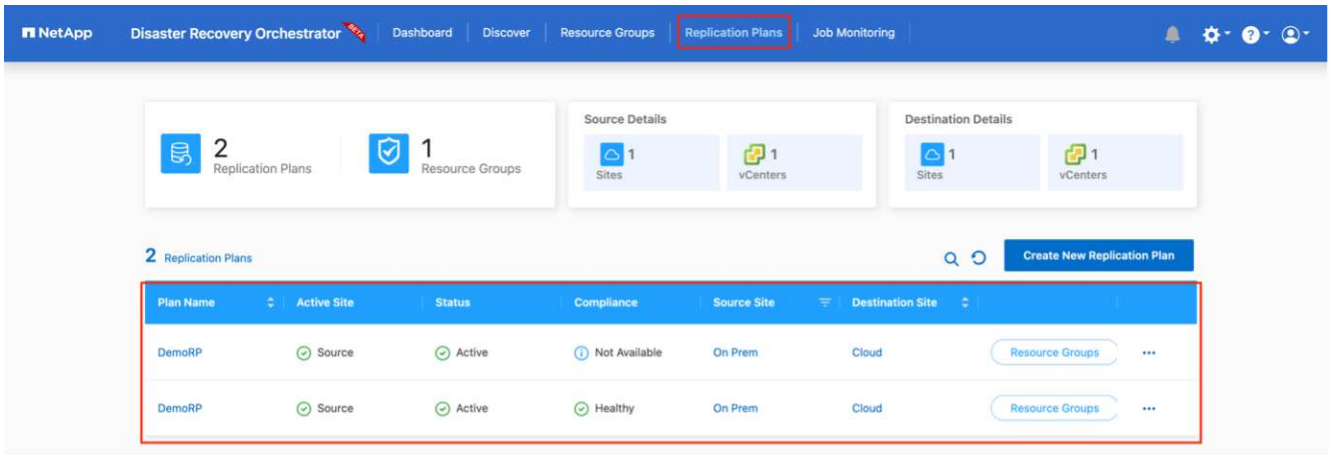
SnapMirror è al livello del volume. Pertanto, tutte le VM vengono replicate nella destinazione di replica. Assicurati di selezionare tutte le VM che fanno parte del datastore. Se non vengono selezionate, vengono elaborate solo le VM che fanno parte del piano di replica.



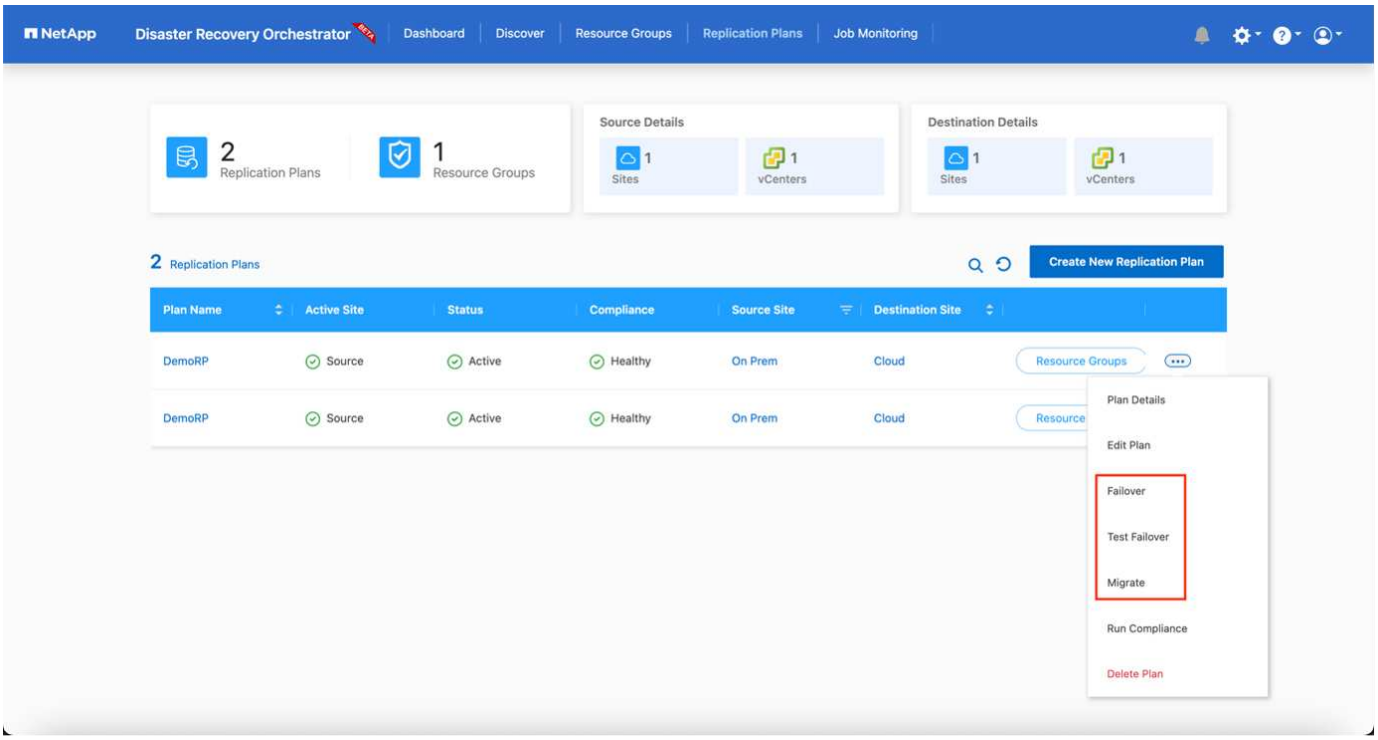
8. Nei dettagli della VM è possibile ridimensionare facoltativamente i parametri CPU e RAM della VM; questa opzione può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o per eseguire test DR senza dover predisporre un'infrastruttura VMware fisica uno a uno. Inoltre, è possibile modificare l'ordine di avvio e il ritardo di avvio (secondi) per tutte le VM selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche rispetto a quelle selezionate durante la selezione dell'ordine di avvio del gruppo di risorse. Per impostazione predefinita, viene utilizzato l'ordine di avvio selezionato durante la selezione del gruppo di risorse; tuttavia, è possibile apportare modifiche in questa fase.

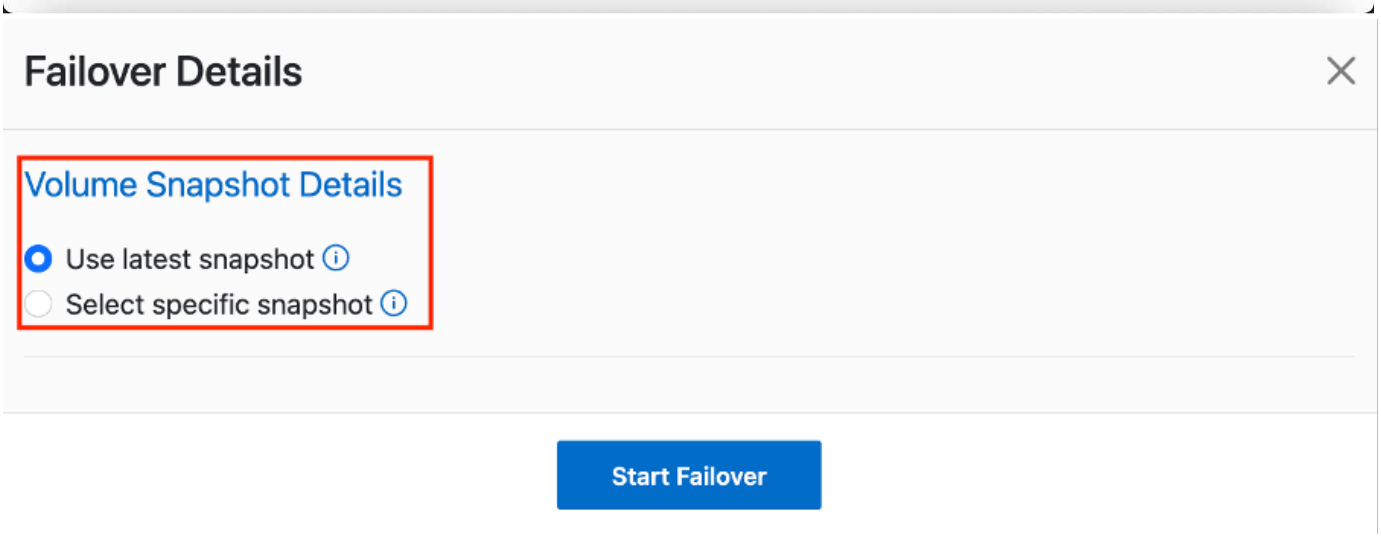


9. Fare clic su **Crea piano di replicazione**.

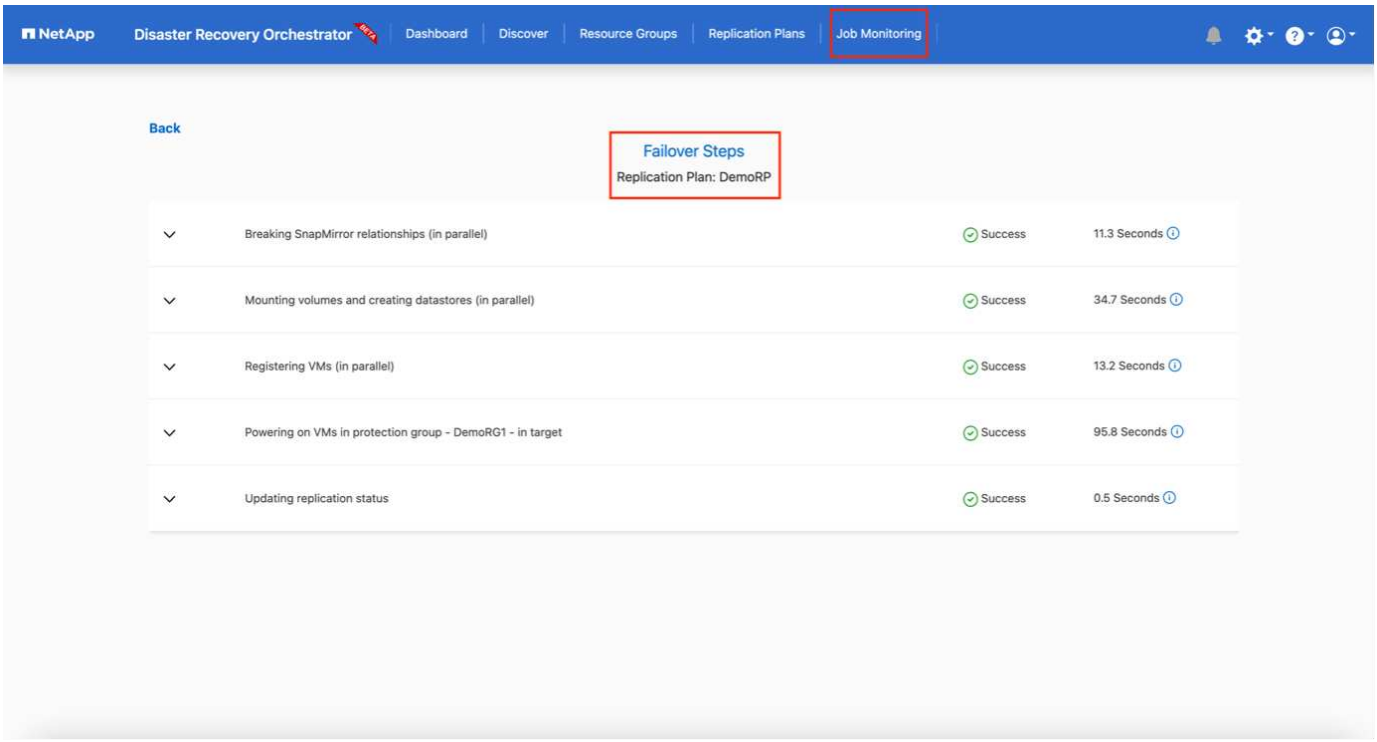


Dopo aver creato il piano di replicazione, è possibile utilizzare l'opzione failover, l'opzione test-failover o l'opzione migrazione, a seconda dei requisiti. Durante le opzioni di failover e test-failover, viene utilizzata la copia Snapshot SnapMirror più recente oppure è possibile selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (in base ai criteri di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come un ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i punti disponibili nel tempo. Per attivare il failover o il failover di prova con la configurazione specificata nel piano di replica, è possibile fare clic su **Failover** o **Failover di prova**.

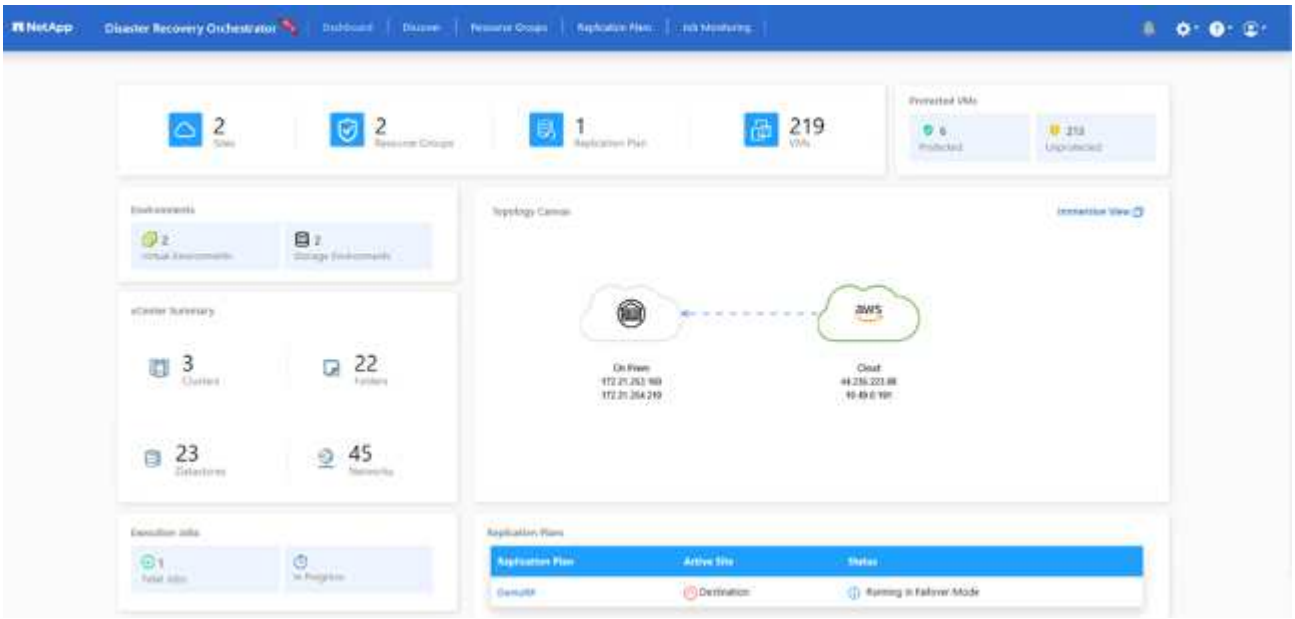




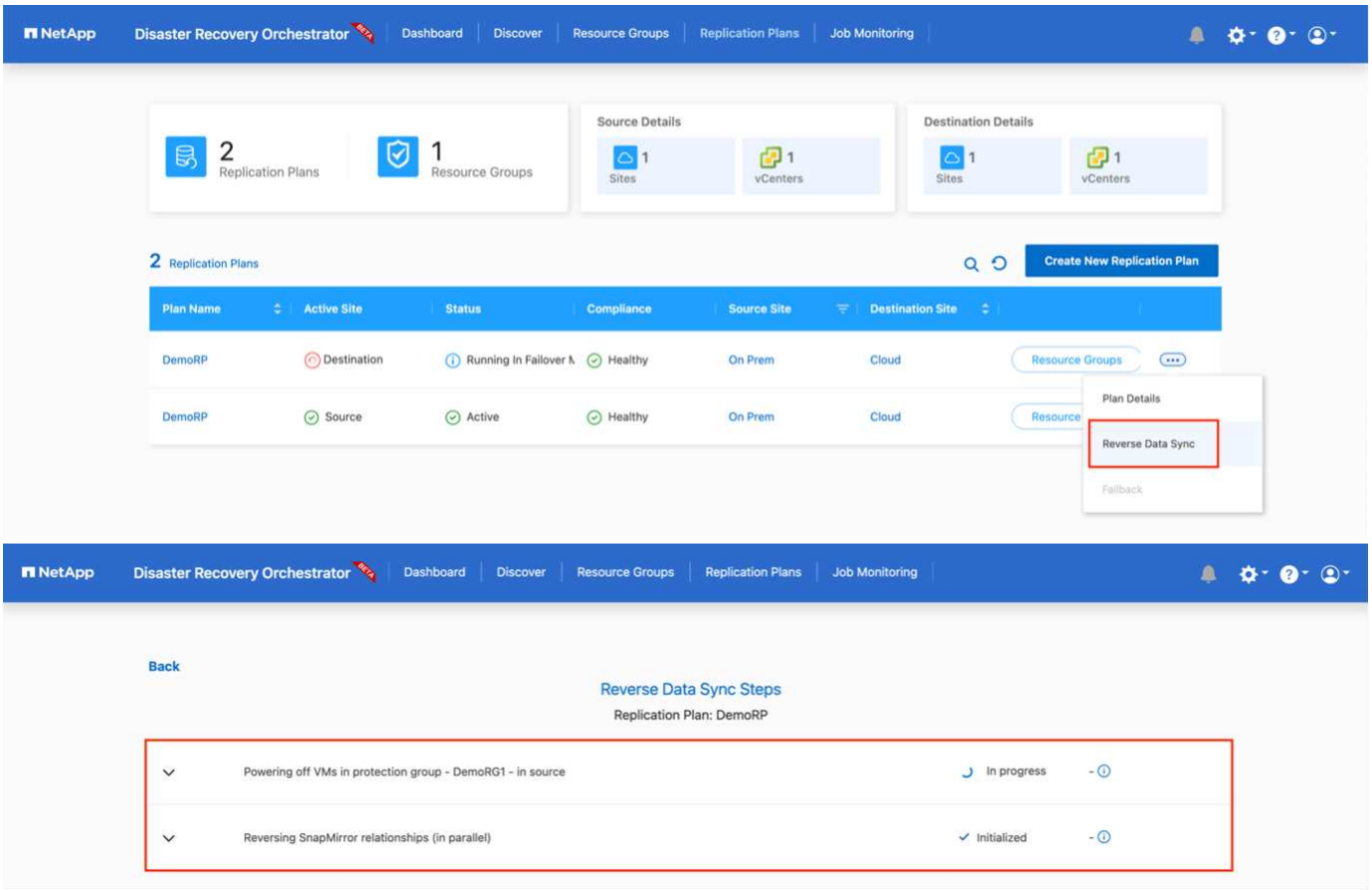
Il piano di replicazione può essere monitorato nel menu delle attività:



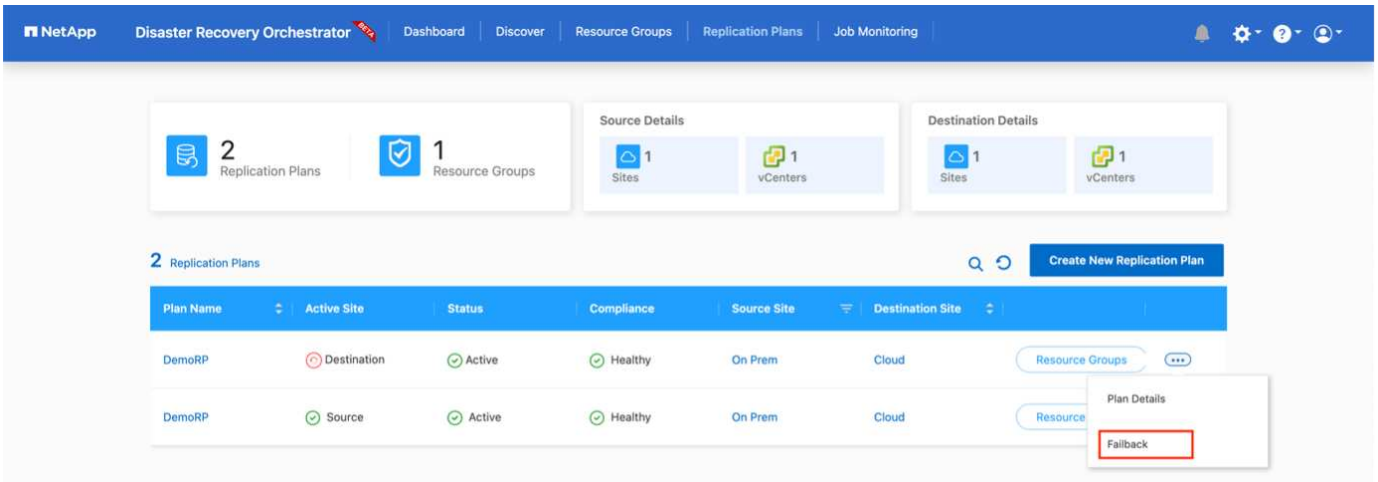
Dopo l'attivazione del failover, gli elementi recuperati possono essere visualizzati nel VMC vCenter (VM, reti, datastore). Per impostazione predefinita, le VM vengono ripristinate nella cartella Workload.

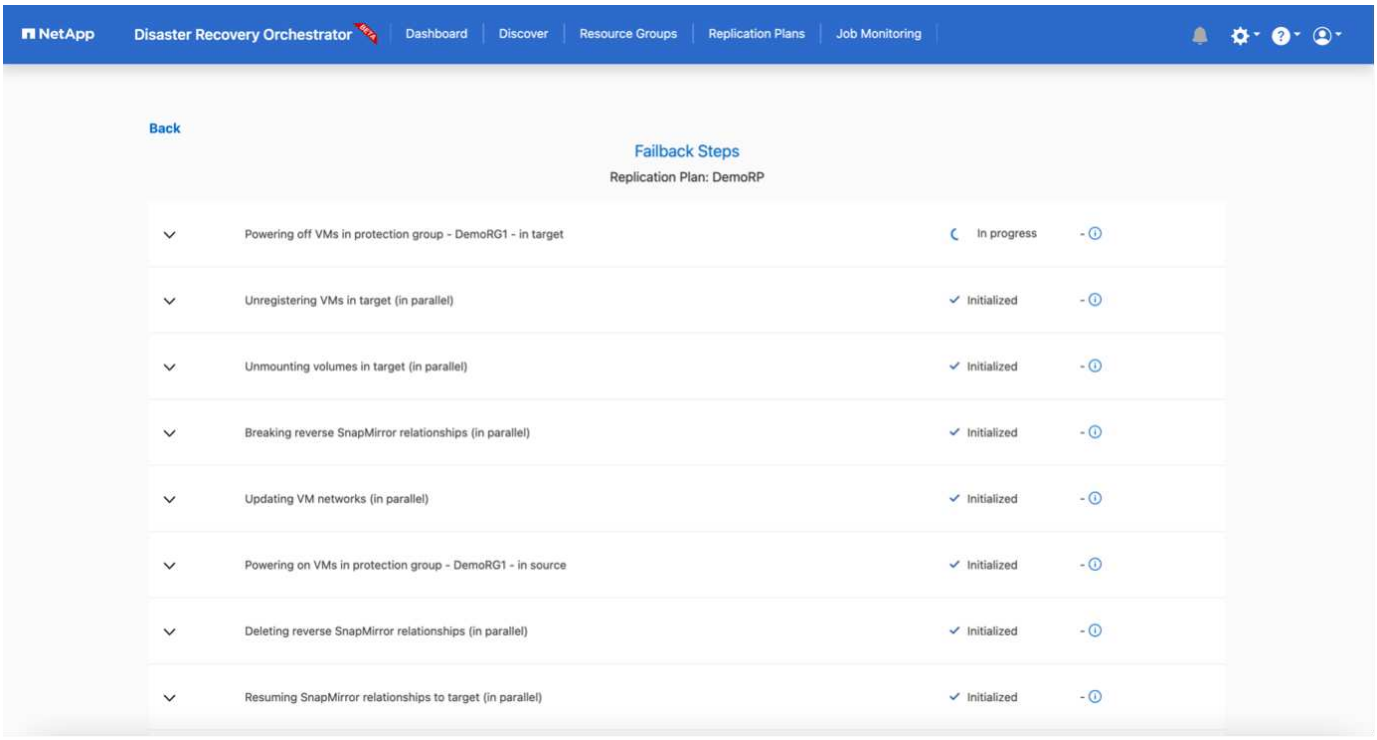


Il failback può essere attivato a livello del piano di replicazione. Per un failover di test, è possibile utilizzare l'opzione tear-down per annullare le modifiche e rimuovere la relazione FlexClone . Il failback correlato al failover è un processo in due fasi. Selezionare il piano di replicazione e selezionare **Sincronizzazione dati inversa**.

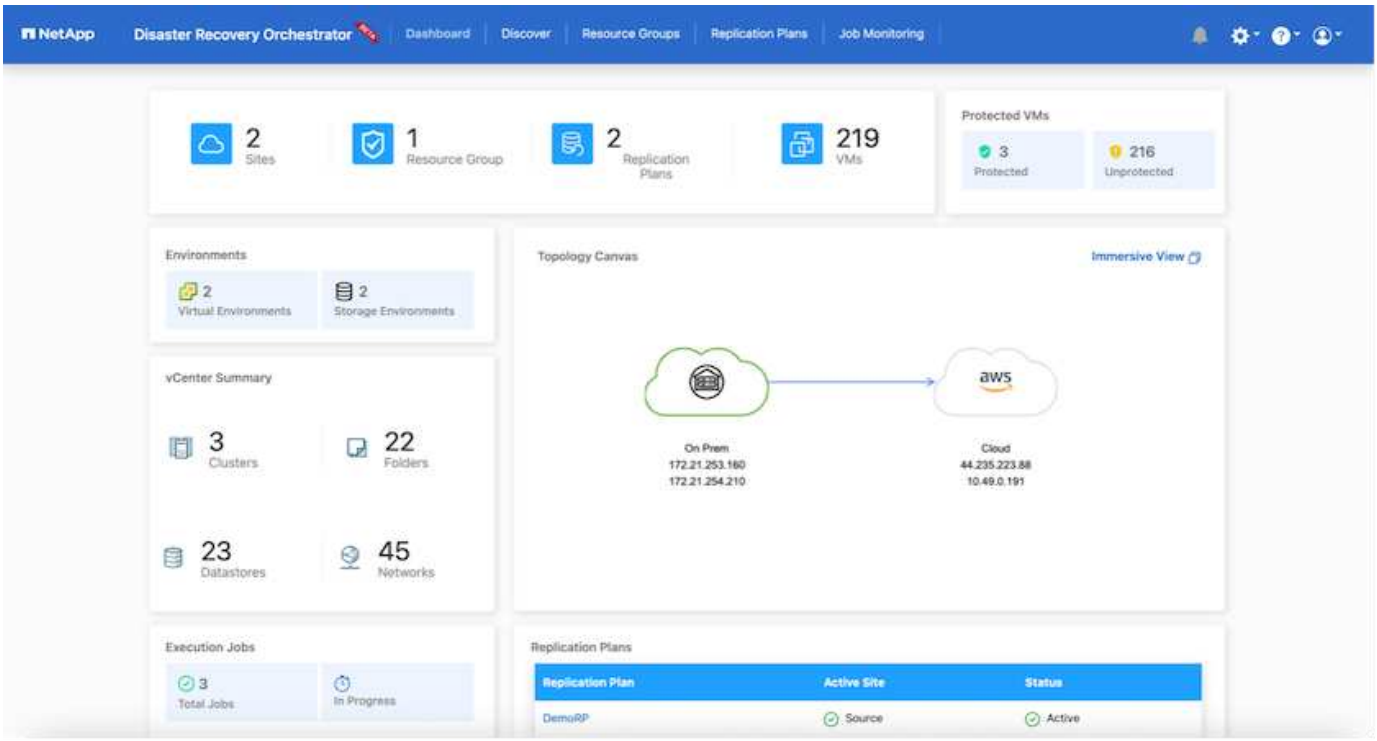


Una volta completato, è possibile attivare il failback per tornare al sito di produzione originale.





Da NetApp BlueXP, possiamo vedere che lo stato di replicazione si è interrotto per i volumi appropriati (quelli che erano stati mappati su VMC come volumi di lettura-scrittura). Durante il failover di prova, DRO non mappa il volume di destinazione o di replica. Al contrario, crea una copia FlexClone dell'istanza SnapMirror (o Snapshot) richiesta ed espone l'istanza FlexClone , che non consuma ulteriore capacità fisica per FSx ONTAP. Questo processo garantisce che il volume non venga modificato e che i processi di replica possano continuare anche durante i test DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che, se si verificano errori o vengono recuperati dati danneggiati, il ripristino può essere ripulito senza il rischio che la replica venga distrutta.



Recupero da ransomware

Recuperare i dati da un ransomware può essere un compito arduo. Nello specifico, può essere difficile per le organizzazioni IT individuare con precisione il punto di ritorno sicuro e, una volta determinato, proteggere i carichi di lavoro recuperati da attacchi ricorrenti, ad esempio da malware inattivi o applicazioni vulnerabili.

DRO risolve questi problemi consentendoti di ripristinare il tuo sistema da qualsiasi momento disponibile. È anche possibile ripristinare i carichi di lavoro su reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro in una posizione in cui non siano esposte al traffico nord-sud. In questo modo, il tuo team addetto alla sicurezza avrà a disposizione un luogo sicuro in cui svolgere analisi forensi e assicurarsi che non vi siano malware nascosti o inattivi.

Benefici

- Utilizzo della replica efficiente e resiliente SnapMirror .
- Ripristino in qualsiasi momento disponibile con conservazione della copia Snapshot.
- Automazione completa di tutti i passaggi necessari per ripristinare centinaia o migliaia di VM dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- Ripristino del carico di lavoro con la tecnologia ONTAP FlexClone utilizzando un metodo che non modifica il volume replicato.
  - Evita il rischio di danneggiamento dei dati per volumi o copie Snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.
  - Potenziale utilizzo dei dati DR con risorse di cloud computing per flussi di lavoro che vanno oltre il DR, come DevTest, test di sicurezza, test di patch o aggiornamento e test di correzione.
- Ottimizzazione di CPU e RAM per contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.